CNews FORUM 2017:
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ЗАВТРА

КАК ЗАЩИТИТЬ КОМПАНИЮ ОТ УТРАТЫ ДАННЫХ СОТРУДНИКОВ

ИВАН АВГУСТОН
ДИРЕКТОР ДЕПАРТАМЕНТА ИТ ГК QBF

QBF

2017

Иван Августон - профайл

QBF

2011 -2017 - Директор ИТ инвестиционной группы компаний QBF

В инвестиционную Группу компаний QBF Иван пришел в 2011 году и большую часть своей карьеры строил параллельно с развитием корпорации.
На данный момент Иван отвечает за организацию, планирование, контроль и управление всеми ИТ-структурами ГК QBF.
Также в список его компетенций входит digital и интернет-продвижение услуг корпорации.

Образование

Российский государственный университет нефти и газа имени И.М. Губкина, специализация «Техника и технология поиска и разведки УВ», 2009г.

Инвестиционная компания QBF

Инвестиционная Группа компаний QBF предоставляет услуги по управлению активами на финансовых рынках Северной Америки, Европы, России с 2008 года.

Филиалы и представительства компании QBF:
Москва, Санкт-Петербург, Екатеринбург, Тюмень, Калининград.

Направления деятельности ГК QBF:

- Стратегии управления активами на российском и зарубежном финансовых рынках
- Структурные продукты
- Специализированные инвестиционные услуги (EAM / EAM+, REPO SWISS, валютное хеджирование)
- Консультационное управление
- Инвестиции в недвижимость

Награды и рейтинги ГК QBF

ОБЩЕСТВЕННАЯ ПРЕМИЯ «ФИНАНСОВАЯ ЭЛИТА РОССИИ»

«Стратегия доверительного управления» - 2017

«Антикризисная стратегия года» - 2016

SPEAR'S RUSSIA WEALTH MANAGEMENT AWARDS

Дмитрий Кипа - Лучший инвестиционный консультант - 2016

Лучшая инвестиционная компания года — 2015, 2014

Старт года - 2013

РЕЙТИНГИ РА ЭКСПЕРТ

Рейтинг Привлекательности Работодателя — A.Hr, 2015

РЕЙТИНГ ПОРТАЛА HH.RU

«3 место в рейтинге работодателей “Финансовый сектор" — 2015»

Как защитить компанию от утраты данных сотрудников

QBF

I. О каких данных идет речь?
   - Документы Microsoft (Бухгалтерия, Юристы, Канцелярия, Кадры)
   - Электронная почта
   - Базы данных

II. Какие угрозы влияют на данные?
   - Шифровальщики
   - Аппаратные сбои HDD
   - Атаки на сервера (SPAM, DDOS, root-kit)
   - Конкурентная разведка

III. А что в облаках?
   - Все выше перечисленное
   - Угрозы связанные с доступом к данным администраторов ЦОД
   - Угрозы выхода из строя ЦОД

По данным исследований в Америке, компании, потерявшие свои данные за последние сутки в течении года, становились банкротами.

Программы

QBF

docker

Active Directory

ZABBIX

NGINX

BRO NETWORK SECURITY MONITOR

MySQL

APACHE
HTTP SERVER

SALTSTACK

Microsoft System Center

Microsoft SharePoint 2010

redhat
RED HAT
ENTERPRISE VIRTUALIZATION

Оборудование

QBF

Техническая и административная защита

- Сегментация на подсети
- Контроль трафика между сегментами
- Токены доступа к АРМ и орг. Технике
- Контроль мессенджеров и электронной почты
- Контроль доступа съёмных устройств
- Контроль доступа к локальной сети
- AppLocker
- SCDPM
- СКУД (Доступ к АРМ только после входа в кабинет)

- Регламенты и положения
- Корпоративные съемочные носители
- Изменения в должностные инструкции
- КТ
- Регламент на использование КТО

Пирамида ценности данных компании

Принято считать, что в основном инсайдеры действуют исключительно из-за желания заработать на продаже корпоративных секретов.

К сожалению, не всё так просто – очень часто оказывается, что корпоративными секретами делятся те, кого работодатель и так не обижал в финансовом плане, не получая при этом никакой материальной выгоды.

Мотивация инсайдера – один из основных ключей к его выявлению и обезвреживанию. Фактически, без понимания причин того, почему тот или иной сотрудник распространяет закрытую корпоративную информацию, достаточно трудно вывести его «на чистую воду» в сжатые сроки.

http://dehack.ru/arts/kak_raspoznat_insajdera_/

Маркеры подозрительной активности

- Логи сервера с неправильными паролем
- Трафик запроса 404 страницы
- Прямая разведка сети, сетевые карты в неразборчивом режиме
- Рост трафика deny на маршрутизаторе локальной сети
- SNMP запросы
- Рост исходящего трафика, сигнатуры передачи «тяжелых» данных
- Подозрительный трафик на стандартных портах 80 443 25 993 135 445
- Рассылка писем с доверенных адресов, содержащие файлы, либо ссылку с неявным призывом перейти, либо запустить файл (DLP)